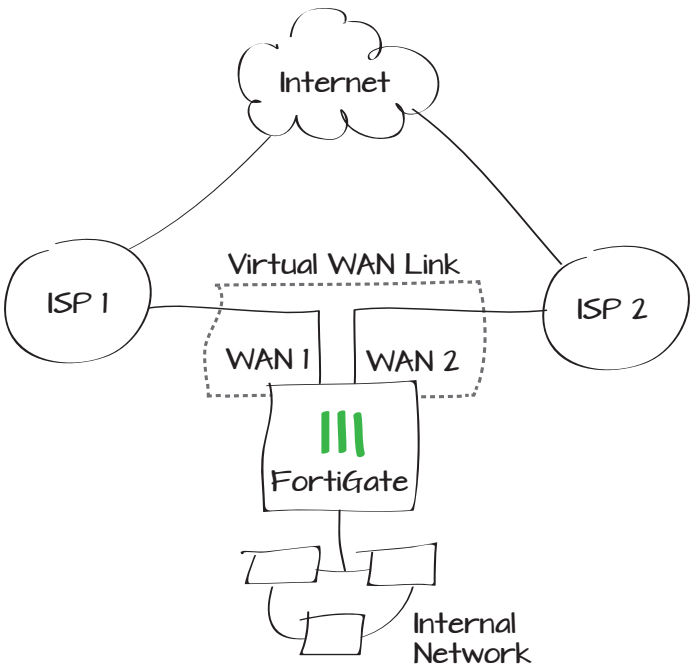
Using a virtual WAN link for redundant Internet connections

In this example, you will create a virtual WAN link that provides your FortiGate unit with redundant Internet connections from two Internet service providers (ISPs). The virtual WAN link combines these two connections into a single interface.

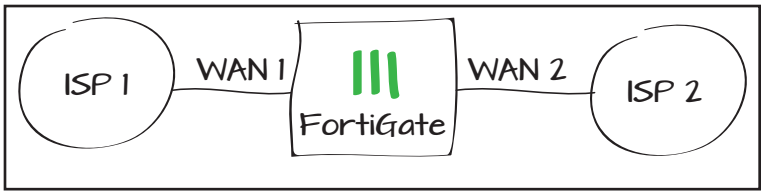
This example includes weighted load balancing so that most of your Internet traffic is handled by one ISP.

1. Connecting your ISPs to the FortiGate
2. Deleting security policies and routes that use WAN1 or WAN2
3. Creating a virtual WAN link
4. Creating a default route for the virtual WAN link
5. Allowing traffic from the internal network to the virtual WAN link
6. Results



Connecting your ISPs to the FortiGate

Connect your ISP devices to your FortiGate so that the ISP you wish to use for most traffic is connected to WAN1 and the other connects to WAN2.



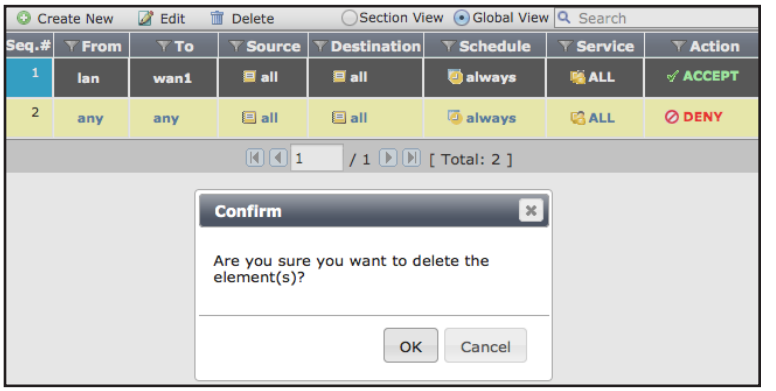
Deleting security policies and routes that use WAN1 or WAN2

You will not be able to add an interface to the virtual WAN link if it is already used in the FortiGate's configuration, so you must delete any policies or routes that use either WAN1 or WAN2.

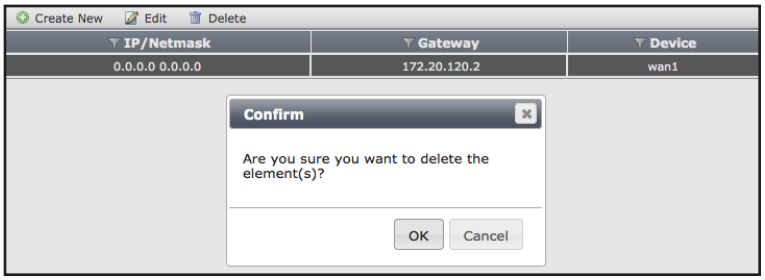
Many FortiGate models include a default Internet access policy that uses WAN1. This policy must also be deleted.

Go to **Policy & Objects > Policy > IPv4** and delete any policies that use WAN1 or WAN2.

After you remove these policies, traffic will no longer be able to reach WAN1 or WAN2 through the FortiGate.

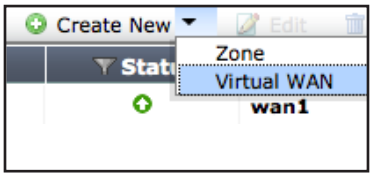


Go to **Router > Static > Static Routes** and delete any routes that use WAN1 or WAN2.

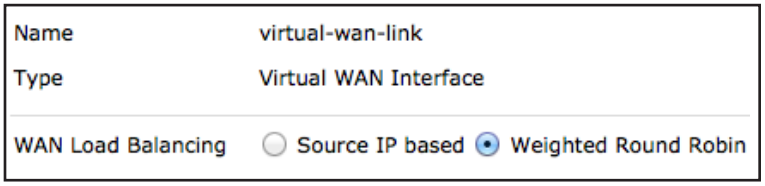


Creating a virtual WAN link

Go to **System > Network > Interfaces** and select **Create New > Virtual WAN**.



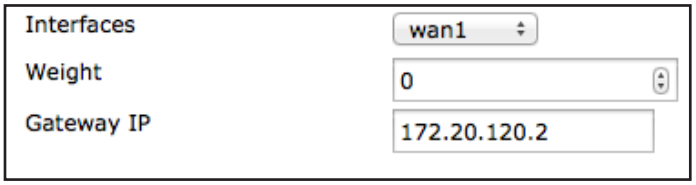
Set **WAN Load Balancing** to **Weighted Round Robin**. This will allow you to prioritize the WAN1 interface so that more traffic uses it.



Add WAN1 to the list of **Interface Members**, set **Weight** to 3, and set it to use the **Gateway IP** provided by your ISP.

Do the same for WAN2, but instead set **Weight** to 1.

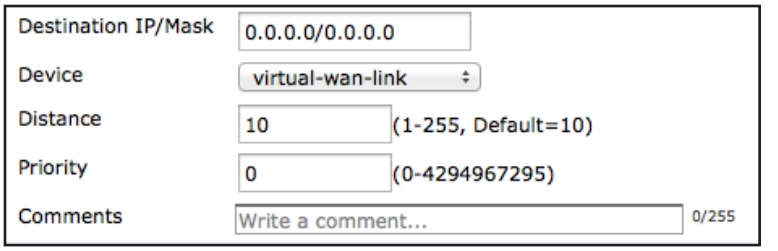
The weight settings will cause 75% of traffic to use WAN1, with the remaining 25% using WAN2.



Creating a default route for the virtual WAN link

Go to **Router > Static > Static Routes** and create a new default route.

Set **Device** to the virtual WAN link.

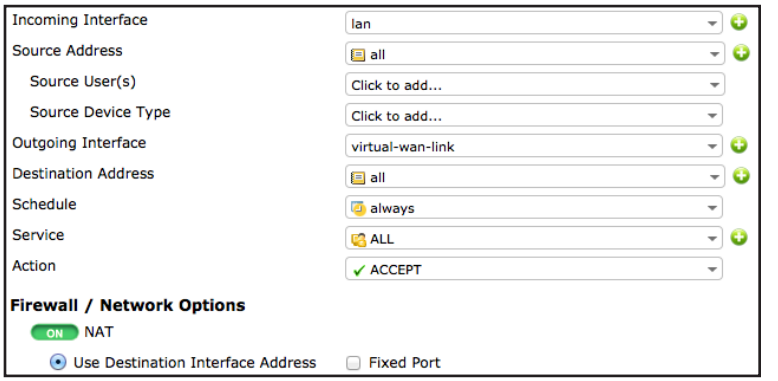


Allowing traffic from the internal network to the virtual WAN link

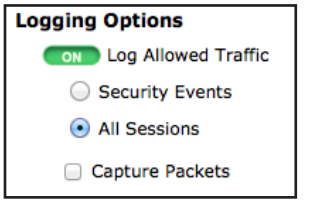
Go to **Policy & Objects > Policy > IPv4** and create a new policy.

Set **Incoming Interface** to your internal network's interface and set **Outgoing Interface** to the virtual WAN link.

Turn on **NAT**.



Scroll down to view the **Logging Options**. To view the results later, turn on **Log Allowed Traffic** and select **All Sessions**.

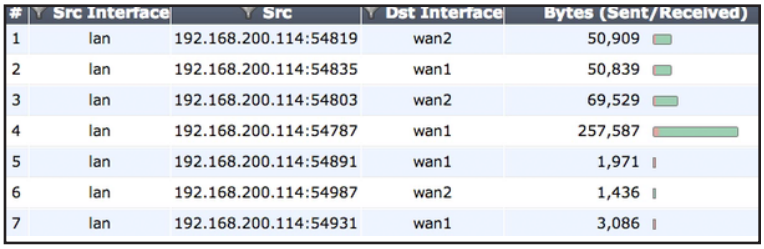


Results

Browse the Internet using a PC on the internal network and then go to **System > FortiView > All Sessions**.

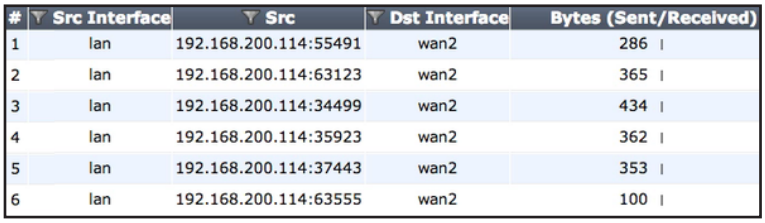
Ensure that the **Dst Interface** column is visible in the traffic log. If it is not shown, right-click on the title row and select **Dst Interface** from the dropdown menu. Scroll to the bottom of the menu and select **Apply**.

The log shows traffic flowing through both WAN1 and WAN2.



#	Src Interface	Src	Dst Interface	Bytes (Sent/Received)
1	lan	192.168.200.114:54819	wan2	50,909
2	lan	192.168.200.114:54835	wan1	50,839
3	lan	192.168.200.114:54803	wan2	69,529
4	lan	192.168.200.114:54787	wan1	257,587
5	lan	192.168.200.114:54891	wan1	1,971
6	lan	192.168.200.114:54987	wan2	1,436
7	lan	192.168.200.114:54931	wan1	3,086

Disconnect the WAN1 port, continue to browse the Internet, and refresh the traffic log. All traffic is now flowing through WAN2, until you reconnect WAN1.



#	Src Interface	Src	Dst Interface	Bytes (Sent/Received)
1	lan	192.168.200.114:55491	wan2	286
2	lan	192.168.200.114:63123	wan2	365
3	lan	192.168.200.114:34499	wan2	434
4	lan	192.168.200.114:35923	wan2	362
5	lan	192.168.200.114:37443	wan2	353
6	lan	192.168.200.114:63555	wan2	100